Amendments to the Claims

1. (CURRENTLY AMENDED) A method of verifying the knowledge of a secret number s in a prover device~~(10)~~ by a verifier device~~(30)~~ having no knowledge of the secret number, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein.

2. (ORIGINAL) The method of claim 1 in which the zero knowledge protocol is the Fiat-Shamir protocol.

3. (ORIGINAL) The method of claim 1 in which the zero knowledge protocol is the Guillou-Quisquater protocol.

4. (CURRENTLY AMENDED) The method of claim 2 including the steps of:

(i) providing~~(102)~~ to the verifier device~~(10)~~ a value $v = s^2$ being the Montgomery multiplication of the secret number s by itself;

(ii) computing~~ (106)~~, by the prover device, the value $x = r \times_m r$, where r is a random number and transmitting the value of x to the verifier device;

(iii) selecting~~ (108)~~, by the verifier device, a challenge value of e from the set {0, 1} and transmitting the challenge value to the prover device;

(iv) computing~~ (110)~~, by the prover device, the value $y = r \times_m s^e$ and transmitting the value y to the verifier device; and

(v) the verifier device~~(10)~~ checking the authenticity of the prover's response according to the values of x, y and v previously received and according to the challenge value e.

5. (CURRENTLY AMENDED) The method of claim 4 wherein the step of checking the authenticity of the prover's response comprises the steps of:

for a challenge value of $e = 1$, computing~~(115)~~ the values of $y \times_m y$ and $v \times_m x$ and checking~~(116)~~ that they are the same; or for a challenge value of $e = 0$, computing~~(120)~~ the value of $y \times_m y$ and checking~~(121)~~ that it is the same as the previously received value of x.

6. (CURRENTLY AMENDED) The method of claim 4 ~~or claim 5~~ further including the steps of repeating steps (ii) to (v) for a number of consecutive rounds to confirm the authenticity of the prover device.

7. (CURRENTLY AMENDED) The method of claim 4 ~~or claim 5~~ in which the secret number s is a Montgomery representation of another number s' known in the prover device domain but not in the verifier device domain, further including the step of computing, by the prover device, the value of s from s' according to $s = s'\mathrm{R}\ mod\ n$, where $\mathrm{R} > n$, values of n and R being used by both the prover device and the verifier device.

8. (CURRENTLY AMENDED) The method of claim 4 in which the Montgomery multiplications of $s \times_m s$, $r \times_m r$, and $r \times_m s^e$ are carried out according to the formula $a \times_m b = ab\mathrm{R}^{-1}\ mod\ n$, where $\mathrm{R} > n$, values of n and R being used by both the prover device~~(10)~~ and the verifier device~~ (30)~~.

9. (CURRENTLY AMENDED) The method of claim 5 in which the Montgomery multiplications of $y \times_m y$ and $s^2 \times_m x$ are carried out according to the formula $a \times_m b = ab\mathrm{R}^{-1}\ mod\ n$, where $\mathrm{R} > n$, values of n and R being used by both the prover device~~(10)~~ and the verifier device~~ (30)~~.

10. (ORIGINAL) The method of claim 1 in which all computations in the zero knowledge protocol are performed using Montgomery representation of numbers and using Montgomery multiplication operations.

11. (CURRENTLY AMENDED) The method of claim 3 including the steps of:

(i) providing~~(303)~~ to the verifier device a value s^e being the Montgomery e^{th} power of the secret number s;

(ii) computing ~~(306)~~, by the prover device ~~(10)~~, the value $x = r^e$, being the Montgomery e^{th} power of r where r is a random number, and transmitting the value of x to the verifier device ~~(30)~~;

(iii) selecting ~~(308)~~, by the verifier device, a challenge value of c from the set {0, 1, ... $e - 1$} and transmitting the challenge value to the prover device;

(iv) computing ~~(310)~~, by the prover device, the value $y = r \times_m s^c$ and transmitting~~(311)~~ the value y to the verifier device; and

(v) the verifier device~~(30)~~ checking the authenticity of the prover's response according to the values of x, y and s^e previously received according to the challenge value c.

12. (CURRENTLY AMENDED) The method of claim 11 wherein the step of checking the authenticity of the prover's response comprises the step of:

computing~~(313, 314)~~ the values of y^e and $x \times_m s^{ec}$ and checking that they are the same.

13. (CURRENTLY AMENDED) The method of claim 11 ~~or claim 12~~ further including the steps of repeating steps (ii) to (v) for a number of consecutive rounds to confirm the authenticity of the prover device.

14. (CURRENTLY AMENDED) A prover device~~(10)~~ having contained therein a secret number s in Montgomery representation, the device adapted for proving the knowledge of the secret number s to a verifier device without conveying knowledge of the secret number itself, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein.

15. (CURRENTLY AMENDED) The prover device of claim 14 further including:

means~~(12)~~ for selecting a random number, r;
means~~(11)~~ for computing the Montgomery squareof r to obtain x;
means for transmitting x to a verifier device ~~(30)~~;
means ~~(11)~~ for receiving a challenge value, e;

means ~~(11)~~ for computing the Montgomery product of $y = r \times_m s$; and

means for transmitting y to the verifier device ~~(30)~~.

16. (CURRENTLY AMENDED) The prover device of claim 14 further including:

means ~~(12)~~ for selecting a random number, r;

means ~~(11)~~ for computing the Montgomery e^{th} power of r to obtain x;

means for transmitting x to a verifier device;

means~~(11)~~ for receiving a challenge value, c;

means~~(11)~~ for computing the Montgomery product of $y = r \times_m s$; and

means for transmitting y to the verifier device.

17. (CURRENTLY AMENDED) A verifier device~~(30)~~ for verifying the knowledge of a secret number s in a prover device without knowledge of the secret number itself, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein.

18. (CURRENTLY AMENDED) The verifier device~~(30)~~ of claim 17 further including:

means~~(31)~~ for receiving the Montgomery square v of the secret number s;

means~~(31)~~ for receiving the Montgomery square, x of a random number, r;

means~~(31)~~ for transmitting a challenge value, e to the prover device;

means~~(31)~~ for checking the authenticity of the prover's response, y according to the Montgomery square of y verified against values of x and / or v received from the prover device according to the challenge value, e.

19. (CURRENTLY AMENDED) The verifier device of claim 17 further including:

means for receiving the Montgomery e^{th} power, s^e of the secret number s;

means for receiving the Montgomery e^{th} power, x of a random number, r;

means for transmitting a challenge value, c to the prover device;

means~~(31)~~ for checking the authenticity of the prover's response, *y* according to the Montgomery e^{th} power of *y* verified against the value of $x \times_m s^{ec}$ received from the prover device, according to the challenge value, *c*.

20. (CURRENTLY AMENDED) A method of proving the knowledge of a secret number *s* in a prover device~~(10)~~ to a verifier device~~(30)~~ having no knowledge of the secret number, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein, comprising the steps of:

selecting~~(305)~~ a random number, *r*;
computing~~(306)~~ the Montgomery e^{th} power of *r* to obtain *x*;
transmitting~~(306)~~ *x* to a verifier device;
receiving a challenge value, *c*;
computing~~(310)~~ the Montgomery product of $y = r \times_m s^c$; and
transmitting~~(311)~~ *y* to the verifier device.

21. (CURRENTLY AMENDED) A method of verifying the knowledge of a secret number *s* in a prover device~~(10)~~ by a verifier device~~(30)~~ having no knowledge of the secret number, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein, comprising the steps of:

receiving~~(103)~~ the Montgomery square *v* of the secret number *s*;
receiving~~(107)~~ the Montgomery square, *x* of a random number, *r*;
transmitting~~(108)~~ a challenge value, *e* to the prover device;
checking the authenticity of the prover's response, *y* according to the Montgomery square of *y* verified against values of *x* and / or *v* received from the prover device according to the challenge value *e*.

22. (CURRENTLY AMENDED) A method of verifying the knowledge of a secret number *s* in a prover device~~(10)~~ by a verifier device~~(30)~~ having no knowledge of the secret number, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein, comprising the steps of:

receiving~~(303)~~ the Montgomery e^{th} power of the secret number s;

receiving~~(307)~~ the Montgomery e^{th} power, x of a random number, r;

transmitting~~(308)~~ a challenge value, c to the prover device;

checking~~(315)~~ the authenticity of the prover's response, y according to the Montgomery e^{th} power of y verified against the value of $x \times_m s^{ec}$ received from the prover device according to the challenge value c.

23. (CURRENTLY AMENDED) A computer program product, comprising a computer readable medium having thereon computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the procedure of ~~any one of claims 1 to 13 and 19 to 22~~claim 1.

24. A computer program, distributable by electronic data transmission, comprising computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the procedure of ~~any one of claims 1 to 13 and 19 to 22~~claim 1.

25. (ORIGINAL) Apparatus substantially as described herein with reference to the accompanying drawings.

26. (ORIGINAL) A method substantially as described herein with reference to the accompanying drawings.